PROPOSTA TECNICO ECONOMICA

DESTINATARIO:
Amministrazione Comunale di **GUGLIONESI**
Alla c.a. Dott. Francesco Vernacchia
e-mail | pec francescovernacchia@comune.guglionesi.cb.it

DATA EMISSIONE: 22/09/2025
RIFERIMENTO: BA-ENTSRV **596582/2025**

OGGETTO:
SOLLECITI CANONE IDRICO:
Emissione, stampa, imbustamento, postalizzazione, acquisizione e rendicontazione incassi

RIFERIMENTO MUNICIPIA PER ASPETTI ECONOMICI
ANTONIO GALLUCCI
e-mail antonio.gallucci@eng.it
mobile 348 7111525

Municipia S.p.A
Il Procuratore Speciale

Firmato digitalmente da:
PAOLO DI LEO
Data: 22/09/2025 20:02:00

MUNICIPIA
GRUPPO ENGINEERING
Municipia S.p.A.
Sede legale: 38122 Trento - Via A. Olivetti, 7
Tel. 0461.158501 -Fax 0461.1585039
Codice fiscale 01973900838 – P. IVA 01973900838
R.E.A. TN – 209533 - Registro Imprese Trento 01973900838
Capitale Sociale Euro 13.000.000,00 i.v. - *società con socio unico*
municipia@eng.it – municipia@pec.eng.it
www.municipia.eng.it - www.eng.it
Società soggetta all'attività di direzione e coordinamento
di Engineering Ingegneria Informatica Spa

CAPITOLO 1 - PROPOSTA ECONOMICA

In questo capitolo è indicata la quotazione economica del servizio descritto nel Capitolo 2 Proposta Tecnica

QUOTAZIONE SERVIZI

SERVIZIO PROPEDEUTICO ALLA EMISSIONE DEI DOCUMENTI

DESCRIZIONE	IMPORTO STIMATO
Emissione, stampa, imbustamento, postalizzazione e acquisizione e rendicontazione incassi di ca 600 solleciti del canone idrico (a corpo)	€ 3.000,00

→ MODALITÀ PER L'ACQUISTO DEI SERVIZI SOPRA INDICATI:

La contrattualizzazione per l'adesione ai servizi proposti può avvenire attraverso le piattaforme di approvvigionamento digitali certificate e/o quanto previsto dalle norme vigenti.

SERVIZIO DI POSTALIZZAZIONE CON QUOTAZIONE SEPARATA PER LA NOTIFICA DEI DOCUMENTI

In questa sezione sono indicati i valori economici di PPII attualmente in vigore riferiti al servizio di postalizzazione massiva.

SERVIZIO POSTALIZZAZIONE AVVISI DI PAGAMENTO	IMPORTO STIMATO
Spese Postali Il servizio offerto si completa con l'invio degli atti attraverso il sub-affidamento dei servizi postali, demandato da Municipia a soggetti titolari di idonea licenza ministeriale. I costi sono sostenuti da Municipia Spa e addebitati al Cliente, dietro effettiva rendicontazione, quale rimborso delle spese anticipate per l'invio dei documenti. Si precisa che gli importi indicati sono del tutto indicativi, saranno infatti applicate le tariffe in vigore al momento della postalizzazione effettiva. **Si evidenzia che le spese postali non possono transitare su MEPA in quanto Municipia non è una azienda di recapito. Per tali spese dovrà pervenire apposita determina.**	€ 3.250,00
TOTALE STIMATO	€ 3.250,00

→ MODALITÀ PER L'ACQUISTO I SERVIZI DI POSTALIZZAZIONE

Per quanto riguarda l'adesione ai servizi di postalizzazione l'adesione può essere effettuata tramite determina da inoltrare a: antonio.gallucci@eng.it

TOTALE GENERALE STIMATO	**€ 6.250,00**

Gli importi sopra indicati per i servizi sono espressi in euro e sono da considerarsi al netto di IVA. Ai sensi dell'art. 26 comma 6 del D. Lgs. 81/2008 Municipia Spa dichiara che i costi generali per la sicurezza del lavoro sono già inclusi nei prezzi sopra indicati e sono pari a 0,00 € giorno uomo. Inoltre, i costi per la sicurezza per ridurre i rischi da interferenza sono pari a 0,00€ vista la tipologia intellettuale dell'attività oggetto della fornitura (art.26 comma 5 del D. Lgs. 81/2008).
Gli importi sopra indicati per le spese postali sono espressi in euro e sono da considerarsi esenti da IVA.

Accordo sul trattamento dei dati personali ("DPA" - Data Processing Agreement)

Qualora l'erogazione dei servizi comporti un trattamento da parte di Municipia di dati personali per conto del Cliente, la contrattualizzazione riferita alla presente proposta deve essere corredata dalla sottoscrizione del DPA mediante cui Municipia viene nominata responsabile o sub-responsabile dal Cliente.

n.b. → In assenza di formalizzazione del DPA, Municipia non potrà procedere con l'erogazione di servizi che comportino un trattamento di dati personali per vostro conto.

CAPITOLO 2 - PROPOSTA TECNICA

In questo capitolo è indicata la descrizione del servizio quotato nel Capitolo 1. Proposta Economica che saranno erogati da Municipia in caso di affidamento.

CARATTERISTICHE DEI SERVIZI

SOLLECITI CANONE IDRICO

IL SERVIZIO

Il servizio inizia con l'acquisizione nel gestionale dei dati della lista di carico in formato 290 riferita ai crediti da riscuotere. Prima di procedere con l'emissione dei solleciti vengono effettuate attività ricorrenti atte ad allineare le banche dati e ad aggiornare le informazioni inerenti il debitore come ad esempio l'aggiornamento anagrafico.

Attraverso le fasi elaborative previste dalla procedura di gestione sono predisposti i file per la produzione dei solleciti di pagamento da inoltrare ai contribuenti per i quali non risulta effettuato il versamento di quanto dovuto.

Il layout del documento può essere personalizzato con quanto richiesto dall'Ente (logo, nota informativa, ecc.).

I testi del sollecito nella parte descrittiva sono concordati con l'Ente, comunque, al loro interno riporteranno tutte quelle informazioni minime che caratterizzano gli elementi di trasparenza nei confronti dei Contribuenti.

Il sollecito è corredato dai modelli di pagamento PagoPa.

I flussi contenenti i dati per l'emissione e la notifica dei solleciti sono inoltrati ad apposito "stampatore" convenzionato che procede anche alla notifica dei documenti tramite PPTT.

Per queste attività viene fornito il supporto per l'acquisizione e la rendicontazione delle notifiche.

Con scadenza mensile viene fornita la rendicontazione degli incassi acquisirti in procedura.

CAPITOLO 3 - CONDIZIONI SPECIFICHE DI FORNITURA

In questo capitolo sono indicate le condizioni specifiche di fornitura per l'erogazione dei servizi oggetto della presente proposta tecnico economica.

OBBLIGO DI RISERVATEZZA

Le informazioni contenute nel presente documento devono ritenersi strettamente confidenziali.
Il Cliente è tenuto, pertanto, a:

- non utilizzarle per finalità diverse dalla valutazione della proposta
- non divulgarle e a fare in modo che non vengano divulgate direttamente o indirettamente a soggetti diversi dal proprio personale direttamente coinvolto nella valutazione della stessa
- non copiarle, riprodurle, duplicarle, senza il preventivo consenso scritto di Municipia S.p.A.

OGGETTO DELLA FORNITURA

L'oggetto della fornitura è l'erogazione da parte di Municipia dei servizi / soluzioni descritti nel capitolo 2 Proposta Tecnica e/o negli allegati che costituiscono parte integrante di questa proposta tecnico economica se presenti.

SUBFORNITURA e SUBAPPALTO

Per l'esecuzione della fornitura Municipia potrà avvalersi di operatori economici della rete dei propri partner mediante l'istituto del subappalto previa autorizzazione del Cliente e nei limiti consentiti dalla legislazione vigente nonché delle prestazioni di fornitori in virtù di contratti continuativi nel rispetto dell'art. 119 comma 3 lett. d del Dlgs 36/2023.

OBBLIGHI E RESPONSABILITA' DI MUNICIPIA

Municipia s'impegna a:

- operare con diligenza nello svolgimento di tutte le attività connesse alla Fornitura, mettendo a disposizione personale qualificato all'esecuzione autonoma degli interventi di sua competenza, nel rispetto delle procedure specificate nel presente contratto. Municipia, potrà avviare le lavorazioni a fronte della contrattualizzazione completa (contratto e DPA) da parte del cliente e solo dopo aver ricevuto tutto il materiale necessario per le lavorazioni indicato al punto OBBLIGHI E RESPONSABILITA' DEL CLIENTE.
- operare nel rispetto delle norme particolari di sicurezza e/o riservatezza concordate con il Cliente.
- garantire il rispetto di dette norme di sicurezza e/o riservatezza da parte di terze parti coinvolte nell'espletamento della Fornitura.
- garantire la corretta esecuzione di quanto previsto nel presente contratto, ritenendosi in ogni caso sollevato da ogni responsabilità per eventuali ritardi dovuti a cause di forza maggiore.
- farsi carico di tutti gli oneri sociali ed assicurativi per il personale impiegato nello svolgimento della Fornitura, con particolare riguardo all'assicurazione contro gli infortuni sul lavoro
- garantire l'interoperabilità del servizio SaaS e la portabilità del servizio e dei dati, come previsto dalle norme vigenti
- a restituire al Cliente, in caso di richiesta, gli archivi di propria competenza in formato CSV corredato del relativo tracciato dati. È possibile, su richiesta, avere anche l'esportazione della banca dati direttamente nel formato nativo dell'applicazione. L'eventuale supporto alla corretta lettura dei dati forniti sarà erogato previa quotazione delle giornate di lavoro necessarie a fronte delle quali sarà emessa apposita fatturazione.

OBBLIGHI E RESPONSABILITA' DEL CLIENTE

Il Cliente s'impegna a:

- rendere disponibili tutte le informazioni necessarie per il corretto svolgimento della Fornitura.
- compilare e restituire firmato il documento ricevuto dal ns. Centro Servizi per l'avviamento dei lavori e l'esecuzione delle attività
- consentire l'accesso alle proprie sedi da parte delle persone di Municipia preposte all'erogazione della Fornitura, come pure ai sistemi che devono interoperare con la soluzione SaaS
- rendere evidente a Municipia la copertura del prodotto software standard, cui la Fornitura è connessa, con un contratto di manutenzione, in corso di validità, stipulato con il produttore del software
- mantenere il proprio personale aggiornato sulle evoluzioni dei prodotti oggetto di assistenza da parte di Municipia, e mantenere aggiornate le versioni dei prodotti applicativi e di base in uso, perlomeno alla penultima versione supportata dal produttore del software standard

Il Cliente deve inoltre assicurare, a proprio carico:

- la disponibilità di una connessione internet "Always on" a banda larga che consenta l'operatività "call back", allo scopo di permettere ai tecnici di Municipia l'accesso remoto al sistema del Cliente in qualsiasi momento si renda necessario
- la predisposizione di adeguati strumenti per l'accesso remoto per interventi di assistenza tempestivi ed efficienti.

REQUISITI PRELIMINARI PER ESECUZIONE DEI LAVORI

Per la corretta esecuzione del servizio è obbligatorio che il Cliente:

- nomini il proprio referente interno, quale interlocutore unico, che sarà dedicato a intrattenere i rapporti con la ns. Direzione Tecnica
- fornisca i documenti di "attivazione lavori" debitamente compilati e sottoscritti (laddove previsti)
- rispetti le tempistiche indicate nelle schede tecniche per la fornitura dei flussi informativi oggetto della fornitura (laddove previsti)

DURATA OFFERTA

L'offerta ha una validità di 60 gg. a partire dalla data della presente.

ADESIONE – DURATA - RECESSO

L'**adesione** al servizio può essere contrattualizzata in relazione a quanto indicato nel Capitolo 1 Proposta Economica.
Per la **durata** del **servizio** Municipia si impegna a erogare il servizio oggetto di fornitura nel rispetto delle scadenze e termini previsti dalla normativa vigente a cui il servizio stesso fa riferimento e comunque non oltre 6 mesi dal ricevimento da parte dell'Ente dell'ordine e di tutto il materiale necessario al suo svolgimento.
In caso di **recesso**, per la cui disciplina vige quanto stabilito dalle normative vigenti nonché dalle condizioni generali di contratto relative alle piattaforme di approvvigionamento, il cliente potrà scrivere una PEC al seguente indirizzo: **municipia.supportovendita@pec.it.**

CORRISPETTIVI – FATTURAZIONE – PAGAMENTI

I **corrispettivi** riferiti all'erogazione del/i servizio/i sono indicati nel capitolo della proposta economica e sono riportati al netto di IVA.
Gli importi dovuti dal Cliente per il **servizio** oggetto della presente offerta saranno **fatturati** al termine dei lavori affidati in service.
Per quanto riguarda **le spese postali,** come già indicato nella sezione della Proposta Economica – Capitolo 1., le stesse saranno fatturate a rimborso di quanto anticipato da Municipia nell'ambito del servizio dietro rendicontazione.
In conformità con il D.lgs. 192/2012 **i pagamenti** dovranno essere effettuati tramite Bonifico Bancario entro 30 giorni data fattura.
In caso di ritardato pagamento Municipia si riserva il diritto di sospendere l'esecuzione dei servizi fino ad avvenuto pagamento senza che ciò comporti inadempimento e/o alcuna responsabilità nei confronti del Cliente, e gli interessi moratori ai sensi dell'art. 4 del suddetto D.lgs. decorrono, senza che sia necessaria la costituzione in mora, dal giorno successivo alla scadenza del termine di pagamento. Il tasso dell'interesse di mora (art. 5 del Dlgs 231/2002 modificato dal Dlgs 192/2012) è pari al saggio di interesse del principale strumento di rifinanziamento della Banca Centrale Europea rilevato il primo giorno di ogni semestre, aumentato di otto punti percentuali.

ESCLUSIONI

Non costituisce oggetto del presente contratto tutto quanto non indicato al Capitolo 2 Proposta Tecnica e/o a quanto non indicato nelle schede tecniche eventualmente allegate alla presente proposta tecnico economica.

COSTI SALUTE E SICUREZZA

Si rimanda a quanto previsto nelle condizioni di acquisto dei Mercati Elettronici e a quanto indicato nel Capitolo 1 Proposta Economica.

CONFORMITA ALLA NORMATIVA IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

Le Parti si impegnano a trattare i dati personali raccolti nel corso *dell'esecuzione del Contratto* nel pieno rispetto del Regolamento (UE) 2016/679, *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati* (di seguito anche solo "**GDPR**"), del D.lgs. 30 giugno 2003, n. 196 e ss.mm.ii., nonché dei provvedimenti delle competenti autorità di controllo, incluso il Garante per la Protezione dei Dati Personali.
In conformità a quanto previsto dal GDPR, tutti i dati personali che verranno scambiati fra le Parti *nel corso dello svolgimento del Contratto* saranno trattati rispettivamente da ciascuna delle Parti per le sole finalità indicate nel Contratto e in modo strumentale all'espletamento dello stesso, nonché per adempiere ad eventuali obblighi di legge, della normativa comunitaria e/o prescrizioni del Garante per la Protezione dei Dati Personali e saranno trattati, con modalità manuali e/o automatizzate, secondo principi di liceità e correttezza ed in modo da tutelare la riservatezza e i diritti riconosciuti, nel rispetto di adeguate **misure di sicurezza (vedi Capitolo 4.)** e di protezione dei dati anche sensibili o idonei a rivelare lo stato di salute, previsti dal Codice Privacy e dal Regolamento UE.
Ciascuna Parte riconosce ed accetta che i dati personali relativi all'altra Parte, nonché i dati personali (es. nominativi, indirizzo email aziendale, ecc.) di propri dipendenti/collaboratori, coinvolti nelle attività di cui al presente Contratto, saranno trattati

dall'altra Parte in qualità di autonomo titolare del trattamento, così come definito nel GDPR, per finalità strettamente funzionali all'instaurazione e all'esecuzione del Contratto stesso e in conformità con l'informativa resa da ciascuna Parte, ai sensi e per gli effetti di cui all'articolo 13 del GDPR , che l'altra Parte si impegna sin da ora a portare a conoscenza dei propri dipendenti/collaboratori nell'ambito delle proprie procedure interne.
L'informativa del Fornitore, che deve essere portata alla conoscenza dei dipendenti/collaboratori del Cliente, è reperibile qui**.**
Nel caso in cui, per l'esecuzione del Contratto, una Parte tratti dati personali per conto dell'altra Parte titolare del trattamento, le Parti si impegnano sin d'ora a stipulare e sottoscrivere un apposito e separato accordo scritto sul trattamento dei dati personali / nomina a responsabile del trattamento ai sensi dell'art. 28 del GDPR. La violazione delle previsioni contenute nel presente articolo espone la Parte inadempiente al risarcimento in favore dell'altra Parte dei danni eventualmente cagionati.
Allo stesso modo, ove dalle dinamiche di esecuzione del contratto emergesse una forma di contitolarità dei trattamenti di dati personali di terzi da parte di entrambe le Parti, queste ultime si impegnano a sottoscrivere, senza alcun onere aggiunto per alcuna Parte, un accordo di contitolarità a norma dell'art. 26 del Regolamento UE da allegarsi al presente contratto e a rispettare gli obblighi di informativa verso gli interessati. La violazione delle previsioni contenute nel presente articolo espone la Parte inadempiente al risarcimento in favore dell'altra Parte dei danni eventualmente cagionati.
Riferimento e-mail: **dpo.privacy@eng.it**

DIRITTI DI POPRIETA' INTELLETTUALE

Il Fornitore, ovvero il terzo licenziante, resta pieno ed esclusivo titolare della proprietà intellettuale e/o industriale (ai sensi e per gli effetti del D.Lgs 10.2.2005, n. 30 e ss.mm., e della L. 22.4.1941, n. 633 come integrata e/o modificata dal D.L. 29.1.1992, n. 518 e relativo regolamento di esecuzione, "Legge sui Diritti di Autore" e/o "Legge"), sulle apparecchiature, programmi per elaboratore e/o software, manuali operativi e relativa documentazione eventualmente resi disponibili od utilizzati per l'erogazione della Fornitura.
L'erogazione da parte del Fornitore della Fornitura non fornisce in alcun modo al Cliente e/o a terzi il titolo a diritti di proprietà intellettuale, che sono e rimangono di esclusiva proprietà del Fornitore e/o dei suoi licenzianti, in tal caso si applicheranno le garanzie dei terzi licenzianti, delle quali il Fornitore darà circostanziata informazione scritta al Cliente, nonché le condizioni di licenza d'uso dei suddetti terzi licenzianti, che il Cliente accetta di rispettare.
In caso di Fornitura avente ad oggetto lo sviluppo e realizzazione di software specificatamente per il Cliente e appositamente remunerato, la proprietà del software e della relativa documentazione resteranno del Cliente che concederà al Fornitore una licenza d'uso gratuita a tempo indeterminato.
In caso di servizi di outsourcing il software applicativo messo a disposizione dal Cliente è e resta di proprietà del Cliente e/o dei suoi licenzianti, fermo restando che al Fornitore sarà concessa dal Cliente licenza d'uso gratuita, ai soli fini dell'esecuzione delle prestazioni previste dal Contratto. Il Cliente terrà il Fornitore pienamente mallevato e indenne da qualsiasi danno, onere, azione o conseguenza pregiudizievole in relazione al suddetto software applicativo utilizzato dal Fornitore per l'esecuzione delle prestazioni, incluso il caso di rivendicazioni di terzi su detto software.
Il Cliente s'impegna a adottare tutte le ragionevoli misure necessarie per tutelare i diritti di proprietà intellettuale del Fornitore sia registrati che non registrati, tra i quali – a titolo esemplificativo - i brevetti, marchi, segni distintivi, invenzioni, disegni e modelli, copyright, software e banche dati, segreti commerciali etc. Il Cliente dovrà tempestivamente comunicare per iscritto al Fornitore la scoperta di qualsiasi uso non autorizzato o violazione dei prodotti o dei diritti sui brevetti, copyright, marchi o altri diritti di proprietà intellettuale del Fornitore associati ai prodotti.

SICUREZZA E PROTEZIONE DELLE INFORMAZIONI IN CLOUD SAAS (valido solo per l'erogazione delle soluzioni in Saas)

CONDIVISIONE DI RESPONSABILITA' PER LA SICUREZZA DELLE INFORMAZIONI

Per quanto riguarda l'assunzione di responsabilità in merito ai ruoli che garantiscono la sicurezza delle informazioni, in particolare per le attività (ove applicabili) relative ad:

- Hardening di sistemi e apparati
- Backup
- Controlli crittografici (ove applicabile)
- Gestione delle vulnerabilità tecniche
- Gestione degli incidenti
- Controllo della conformità tecnica
- Test di sicurezza
- Auditing
- Raccolta delle registrazioni (log)
- Protezione delle informazioni al termine del contratto
- Autenticazione e controllo degli accessi

Si concorda che Cliente e Fornitore sono entrambi responsabili, ciascuno per le aree di propria competenza, che sono desumibili contrattualmente.
In linea generale vale la regola secondo cui l'onere di effettuare le attività che garantiscono la sicurezza delle informazioni spetta a chi detiene le password degli account con privilegi di amministrazione degli ambienti da mettere

in sicurezza. Es.: In un contratto per la fornitura di servizi SaaS, ove il Fornitore fornisce e gestisce un layer applicativo su cui sono installati applicazioni e dati, il Fornitore è responsabile per gli adempimenti di sicurezza applicativa (es. predisposizione di funzionalità di autenticazione, logging, gestione di vulnerabilità applicative, etc.) e garantisce che siano implementate le misure di sicurezza infrastrutturale relative alla gestione degli ambienti virtualizzati che ospitano il layer applicativo. Il Fornitore, inoltre, si avvale di subfornitori qualificati e certificati che mettono a disposizione il layer infrastrutturale di base (in modalità IaaS e Paas), con cui sussistono accordi contrattuali in garanzia dell'adozione di misure di sicurezza adeguate.

PROTEZIONE DELLE INFORMAZIONI del Cliente nell'ambito dei servizi Cloud

GARANZIE

Il Fornitore garantisce ai propri Clienti, oltre all'applicazione delle idonee misure per la protezione dei dati personali previste dalla normativa vigente RE UE 679/2016, anche l'applicazione di una serie di misure idonee alla protezione di tutti i dati, tra cui l'adozione, l'applicazione e la certificazione di conformità della/alla norma di sicurezza volontaria ISO/IEC 27001:2022 "Information technology - Security techniques - Code of practice for information security management" ed il rispetto delle linea-guida:

- ISO/IEC 27018:2019 "Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors."
- ISO/IEC 27017:2015 "Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services.

Si forniscono maggiori informazioni con particolare riferimento ai seguenti controlli:

Gestione delle vulnerabilità tecniche

Le vulnerabilità tecniche vengono gestite ciclicamente tramite un processo di individuazione strumentale delle vulnerabilità sugli asset (la frequenza è proporzionale al livello di esposizione degli asset stessi), gli input dei vendor e dei gruppi di interesse in contatto con i competence center tecnici oltre che da possibili inneschi provenienti da strumenti di monitoring o da segnalazioni utente.

La comunicazione ed il fixing delle vulnerabilità tecniche segue sempre un iter concordato tra le parti e da definire in fase di transition (change management) ed è comunque in funzione della gravità delle vulnerabilità stesse.

Hardening delle macchine virtuali

Le attività di hardening delle macchine virtuali che ospitano ambienti applicativi in SaaS per il Cliente saranno effettuate rispettivamente dal fornitore Saas e dai subfornitori IaaS e Paas, come previsto dai relativi accordi contrattuali.

TRATTAMENTO DELLE INFORMAZIONI

Le informazioni affidate al Fornitore vengono trattate per conto del Cliente secondo quanto previsto dalla giurisdizione di riferimento, che è quella europea ed italiana, solo ed esclusivamente per le finalità contrattualizzate, a meno di specifici ed espliciti accordi con il Cliente stesso.

In particolare, il Fornitore si impegna a non utilizzare le informazioni per finalità commerciali senza autorizzazione esplicita del Cliente e dichiara che tale autorizzazione non è mai precondizione necessaria all'erogazione dei propri servizi.

Le informazioni risiedono:

- **in Italia in uno o più dei Datacenter Engineering** (a meno di differenti specifici ed espliciti accordi con il Cliente) qualora il servizio SaaS si attesti su VCloud fornito da Engineering D.Hub
- **in UE in uno o più dei Datacenter messi a disposizione da altri fornitori di infrastruttura Cloud** (ad es. Amazon WebServices) di cui Municipia si avvale, purché essi siano in possesso delle certificazioni previste per l'accreditamento in Marketplace ACN.

I trattamenti vengono effettuati esclusivamente da personale qualificato, formalmente incaricato ai sensi delle normative Privacy ed istruito in tal senso.

DIFFUSIONE DELLE INFORMAZIONI

In caso di richiesta di consegna da parte di Autorità Giudiziarie o Amministrative (es. Polizia, Carabinieri, Guardia di Finanza, Magistratura), delle informazioni affidate al Fornitore dal Cliente, il Fornitore fornirà al Cliente tempestiva notifica di tale richiesta, tranne nei casi di divieto da parte dell'Autorità stessa.

NOTIFICA DEGLI INCIDENTI

Il Fornitore, in armonia alla procedura di Gruppo per la gestione degli incidenti di tipo "data breach" si impegna a notificare tempestivamente al Cliente gli incidenti di sicurezza informatica (data-breach) rilevati tramite strumenti di monitoraggio e controllo o da segnalazioni, che implichino o consistano in:

- Accessi non autorizzati
- Perdita di dati
- Alterazione di dati
- Diffusione indebita di dati

La notifica avverrà via posta elettronica (al riferimento indicato dal Cliente) o secondo le modalità contrattualizzate, di norma entro il giorno successivo alla rilevazione dell'incidente. Successivamente alla sua chiusura, sarà inviato al Cliente l'Incident Report descrittivo dell'accaduto e delle azioni intraprese.

TRASFERIMENTO O RESTITUZIONE DELLE INFORMAZIONI O RIMOZIONE A FINE CONTRATTO

A fine contratto, a seguito della riconsegna dei dati, come descritto nel paragrafo "Obblighi e Responsabilità di Municipia", il Fornitore provvede puntualmente alla cancellazione sicura dei dati cliente, con l'eccezione delle registrazioni che vengono ancora conservate secondo i termini di legge.

UTILIZZO DI SUB-FORNITORI

L'utilizzo di sub-fornitori nell'erogazione dei servizi contrattualizzati è vincolato al consenso esplicito del Cliente (specifica lettera firmata o accettazione del Contratto in cui è contemplato l'utilizzo del sub-fornitore), al quale devono essere resi noti:

- il nome del sub-fornitore
- la/e nazione/i nella quale vengono operati i trattamenti delle informazioni

Nel richiedere tale consenso, Il Fornitore garantisce di aver esteso al sub-fornitore (o al "peer" service provider), le informazioni necessarie al rispetto delle norme per la sicurezza delle informazioni e che il sub-fornitore si sia impegnato a rispettarle.

BACKUP E RESTORE

Il backup dei dati Cliente è finalizzato a consentire il ripristino in caso di eventi avversi.

Il servizio di backup/restore è sempre dovuto dal Fornitore al Cliente tranne nei casi in cui, per natura del servizio o per esplicitazione contrattuale, è il Cliente stesso a provvedere autonomamente.

Il backup dei dati Cliente, qualora dovuto, viene garantito in duplice copia per tutti i dati. Eventuali deroghe richieste dal Cliente possono riguardare ambienti o dati "non di produzione". Originali e copie dei backup vengono conservati in locazioni (fisiche o logiche) differenti e il trasferimento dei dati in sede diversa avviene solo sotto protezione crittografica.

A meno di differenti accordi contrattuali, l'inizio dell'attività di restore dei dati in caso di incidente è sempre garantita, nel caso peggiore, nell'arco del giorno lavorativo successivo all'evento che rende necessario il ripristino. La durata complessiva dell'attività di restore è funzione del volume di dati da ripristinare.

LOGGING

La collezione e conservazione dei log a norma di legge è tipicamente effettuata dal Fornitore, sia direttamente, sia avvalendosi del servizio offerto dai propri sub-fornitori (IaaS e PaaS).

I log vengono resi disponibili al Cliente in forma di report "spot", effettuato su richiesta estemporanea del Cliente oppure, se concordato tra i servizi contrattualizzati, in forma di report periodico, o garantendo l'accesso in visione ai dati via rete. In tutti i casi viene garantita la riservatezza delle informazioni nel senso che ogni Cliente ha visibilità esclusivamente dei log relativi a sistemi/servizi di sua pertinenza.

PROPRIETÀ INTELLETTUALI

Il Fornitore si impegna ad erogare servizi in Cloud utilizzando sistemi con installazioni di licenze valide, ove applicabile.

Reclami di pertinenza del Fornitore saranno indirizzati secondo il processo interno di Gestione dei Reclami.

REVERSIBILITA' DEI SERVIZI SAAS

Per garantire la piena reversibilità del servizio SaaS, forniamo una esportazione completa in formato CSV di tutti i dati afferenti al servizio del cliente. Il file principale può contenere, ai fini di garantire la completa disponibilità di tutti i dati suddetti, un sistema di chiavi esterne di collegamento con eventuali altri file necessari ad una esportazione olistica. All'atto della dismissione il set di dati completo verrà reso disponibile, organizzato come illustrato nel dizionario dati allegato alla fornitura, in formato CSV.

Il processo di reversibilità, studiato con le salvaguardie ed i passi intermedi necessari a garantire l'integrità dei dati di proprietà dell'ente, è costituito delle seguenti fasi:

- Disattivazione delle utenze del cliente ed inibizione all'accesso
- Impostazione della banca dati in sola lettura
- Backup della banca dati in formato nativo
- Esportazione della banca dati in formato CSV
- Fornitura all'ente del link per lo scaricamento della banca dati in formato CSV
- Attesa della conferma di avvenuto download ed integrità dell'esportazione da parte del cliente
- Eliminazione della tenancy del cliente dal servizio SaaS
- Eliminazione del backup in formato nativo
- Eliminazione dell'esportazione in formato CSV

Il processo di reversibilità viene avviato alla cessazione del rapporto con il cliente o durante la vigenza dello stesso, a fronte di specifica richiesta. Al fine di garantire il corretto svolgimento del processo e per garantire la sicurezza del trasporto del dato, Il cliente dovrà inviare a mezzo PEC una comunicazione con la quale fornirà un proprio riferimento, titolato a gestire lato cliente le fasi della procedura, oltre all'indirizzo mail PEC che sarà utilizzato per veicolare i ticket di gestione della procedura di reversibilità. Dall'avvio del processo di reversibilità, il tempo di completamento dello stesso è stimato in 10gg lavorativi. L'eliminazione della tenancy, del backup e dell'esportazione in formato CSV avverranno dopo 10 gg dalla conferma di avvenuto download con esito positivo da parte del Cliente.

CAPITOLO 4 - CONDIZIONI GENERALI DI VENDITA E MISURE DI SICUREZZA

CONDIZIONI GENERALI DI VENDITA

Per quanto non espressamente previsto nel presente documento:

- **per acquisti tramite marketplace (es. MEPA):** si fa espresso rinvio alle condizioni generali di contratto relative al marketplace individuato dall'Ente per l'acquisto
- **per acquisti non effettuati tramite marketplace:** si fa espresso rinvio alla lex specialis di gara e alla normativa vigente.

MISURE DI SICUREZZA

Il contenuto del presente Allegato definisce le misure minime di sicurezza che, ove applicabili, Municipia (di seguito "FORNITORE") si impegna a mantenere attive e rispettare per tutta la durata del Contratto, qualora si trovi ad erogare servizi per e/o verso il Cliente (di seguito "CLIENTE").

Regole Generali Sicurezza	
ID	Clausola
1.1	Il FORNITORE si impegna, per tutte le attività inerenti e riconducibili allo svolgimento delle prestazioni contrattuali, ad adottare politiche aziendali - opportunamente formalizzate e divulgate internamente - coerenti con i contenuti della normativa vigente nonché con i contenuti del presente documento.
1.2	Il FORNITORE deve provvedere al trattamento dei dati in accordo con il loro livello di classificazione, con particolare riferimento alla riservatezza, applicando altresì le politiche eventualmente concordate in tema di data retention.
1.3	Il FORNITORE dà atto e riconosce che i dati delle architetture e delle configurazioni dei sistemi informativi del CLIENTE e/o dei suoi Clienti, con le relative misure di sicurezza, nonché i dati relativi alle vulnerabilità eventualmente riscontrate in occasione dell'esecuzione del Servizio sono informazioni riservate e che dalla loro diffusione all'esterno può derivare un pregiudizio grave, in termini di esposizioni ad attacchi dall'esterno o di riflessi sull'immagine e sulla reputazione.
1.4	Il FORNITORE è tenuto a garantire il rispetto dei livelli di servizio contrattualmente stabiliti con il CLIENTE, anche in casi di emergenza o di contesa delle risorse da parte di altri suoi clienti.
1.5	Il FORNITORE riconosce la proprietà esclusiva dei dati, del software, della documentazione tecnica e normativa e delle risorse ICT del CLIENTE e/o dei suoi Clienti qualora essi vengano utilizzati o comunque resi disponibili per l'erogazione del servizio.
1.6	Il FORNITORE riconosce in qualsiasi momento al CLIENTE il diritto di revocare l'autorizzazione ad effettuare qualunque attività su asset (compresi i dati) del CLIENTE e/o dei suoi Clienti.
1.7	Il FORNITORE si impegna a cancellare in qualunque momento i dati su richiesta del CLIENTE indipendentemente dalla conclusione del rapporto contrattuale.
1.8	Il FORNITORE si impegna a restituire gli asset del CLIENTE (compresi dati, licenze e apparati) nei tempi concordati.
1.9	Il FORNITORE si impegna, qualora un caso di specie non sia contemplato dai controlli previsti, ad applicare le best practice e gli standard riconosciuti in materia.

Personale e organizzazione del FORNITORE	
ID	Clausola
2.1	In relazione al personale comunque coinvolto nell'esecuzione delle obbligazioni contrattuali (ivi compresi collaboratori a qualsiasi titolo), il FORNITORE si impegna, anche ai fini della sicurezza delle informazioni: (a) a garantire che lo stesso abbia qualifiche adeguate per i compiti svolti; (b) a curare che tale personale riceva la necessaria formazione al riguardo e adeguate informazioni sulle regole di cui al precedente punto 1; (c) ad attuare, nell'assegnazione delle mansioni, le opportune politiche di separazione dei compiti; (d) ad attribuire compiti e responsabilità al proprio personale al fine di presidiare le principali minacce interne ed esterne, compreso internet; nei casi di cessazione del rapporto di lavoro o di variazione di incarico, a garantire – tramite processi formalizzati e sicuri - la revoca immediata delle credenziali concesse al proprio personale e la restituzione

Personale e organizzazione del FORNITORE	
ID	Clausola
	degli strumenti assegnati per lo svolgimento delle attività inerenti alle prestazioni contrattuali, come pure di eventuali badge, chiavi e altri strumenti di accesso, identificazione e autenticazione.
2.2	Il FORNITORE si impegna a collaborare con il CLIENTE al fine di assicurare il raccordo con i ruoli e le procedure definite all'interno del CLIENTE per il processo di analisi dei rischi e per il sistema di gestione dei dati. In particolare, il FORNITORE si impegna ad indicare: - un incaricato con il compito di gestire l'attuazione delle disposizioni di sicurezza di questo allegato e di altro dispositivo contrattuale, in possesso di specifiche professionalità e competenze nella materia della sicurezza cibernetica e con adeguato livello di autorità; - un referente tecnico in possesso di competenze tecnico-specialistiche nella materia della sicurezza cibernetica, per lo svolgimento delle funzioni di interlocuzione con le funzioni di sicurezza del CLIENTE ai fini della gestione degli incidenti.
2.3	Il FORNITORE si impegna a tenere: (a) una lista dei luoghi in cui sono ospitati: (i) i dati, (ii) i servizi e (iii) i data center utilizzati dal FORNITORE per la fornitura del Servizio e (b) un documento indicante la gestione degli accessi fisici e logici e il numero di addetti con accesso ai dati del CLIENTE e/o dei suoi Clienti, nonché ad aggiornare regolarmente tale documentazione, consegnandola al CLIENTE, previa richiesta per iscritto.
2.4	Il FORNITORE si impegna tempestivamente a comunicare al CLIENTE la necessità di spostamento delle risorse e dei dati (compresi i backup) da un sito/data center (suo o di terze parti) ad un altro e a implementare nel nuovo centro le stesse misure di sicurezza del sito primario. Resta comunque inteso che lo spostamento delle risorse e dei dati da un sito/data center (suo o di terze parti) ad un altro deve essere preventivamente autorizzato dal CLIENTE. Restano salvi eventuali divieti/restrizioni allo spostamento delle risorse e dei dati eventualmente già previsti nel Contratto.
2.5	Il FORNITORE garantisce che, in caso di subfornitura di attività (che dovrà essere autorizzato e monitorato secondo le modalità previste nel Contratto), tutte le disposizioni relative alla gestione dei dati contenute nel presente Allegato (con particolare riferimento alla riservatezza, retention e cancellazione dei dati) e audit e verifiche siano applicate da tutta la catena di fornitura. Resta inteso che la subfornitura non diminuisce la responsabilità del FORNITORE che è in ogni caso tenuto alla costante verifica e monitoraggio di tali soggetti.
2.6	In presenza di cambi organizzativi del FORNITORE che possano incidere sul livello di integrità, disponibilità e riservatezza dei dati (e comunque in caso di cambio di subfornitori), il FORNITORE dovrà avvertire preventivamente il CLIENTE per consentire le opportune valutazioni e verifiche, anche a mezzo di un audit.
2.7	Il FORNITORE si impegna a non introdurre modifiche (tecnologiche, di organizzazione dei servizi e della catena dei subfornitori) che possano diminuire la sicurezza del Servizio.

Sicurezza fisica e logica del FORNITORE	
ID	Clausola
3.1	Il FORNITORE si impegna a utilizzare per tutti i propri servizi aziendali, inerenti o riconducibili allo svolgimento delle prestazioni contrattuali, misure di sicurezza per la gestione delle credenziali e dei privilegi d'accesso conformi alle norme di legge e che prevedano: (a) utenze univoche e personali; (b) gestione sicura delle credenziali di accesso con scadenza periodica e modifica obbligatoria al primo accesso, garanzia di non riutilizzabilità e storicizzazione nel tempo e controlli automatici di robustezza; (c) criteri e politiche di assegnazione delle credenziali e dei privilegi d'acceso che garantiscano l'adozione del criterio della separazione dei compiti; (d) criteri e politiche di assegnazione dei privilegi d'accesso a garanzia del criterio di minimo privilegio concesso; (e) criteri e politiche di distinzione dei privilegi d'accesso che distinguano le autorizzazioni almeno per accesso ai dati di produzione, accesso e manutenzione dei sistemi, del software e della rete; (f) strumenti e policy di custodia dei supporti e dati ricevuti che prevengano la perdita e l'accesso anche accidentali da terzi.

Sicurezza fisica e logica del FORNITORE	
ID	Clausola
3.2	Il FORNITORE garantisce l'applicazione di misure di sicurezza fisica (quali ad esempio la chiusura dei locali, "clean desk policy", custodia dei supporti consegnati) nelle aree critiche inerenti o riconducibili al servizio fornito (e nei collegamenti da e verso tali sedi). Ove il servizio sia reso nei locali del CLIENTE, il FORNITORE si impegna a far uso corretto delle attrezzature ivi presenti e a segnalare eventuali carenze/malfunzionamenti.
3.3	La distruzione di dati/supporti al termine delle attività contrattualmente previste sarà effettuata tramite procedure e standard che rispettino i requisiti di sicurezza indicati in Contratto e/o comunicati dal CLIENTE.
3.4	Il FORNITORE si impegna ad implementare adeguati meccanismi di isolamento dei dati gestiti per conto del CLIENTE rispetto ai dati gestiti per conto di propri altri clienti a garanzia della loro riservatezza, disponibilità ed integrità.
3.5	Il FORNITORE, su richiesta del CLIENTE, si impegna a inviare una descrizione tecnica dettagliata delle modalità con cui, in esecuzione del Contratto, intende erogare il Servizio e implementare e gestire le misure di sicurezza informatica, fisica ed organizzativa per la protezione degli asset del CLIENTE, atte a garantire un servizio conforme al livello di classificazione richiesto, con particolare riferimento a procedure e strumenti per: (a) la gestione del ciclo di vita (provisioning/deprovisioning) di tutte le credenziali utente e delle relative problematiche di profilazione delle stesse in merito all'accesso a sistemi, applicazioni reti e dati; (b) garantire adeguati livelli di autenticazione, autorizzazione e tracciatura nel caso di accessi da remoto ad asset informativi del CLIENTE e/o dei suoi Clienti; (c) la protezione fisica e logica del Data Center del FORNITORE, nel caso di servizi esternalizzati; (d) la protezione da software malevolo; (e) la gestione delle attività di patching, di security patching, fixing e upgrading di software di base ed applicativo; (f) la gestione e la custodia dei supporti di memorizzazione; (g) la dismissione controllata degli asset con l'adozione di sistemi di cancellazione sicura delle informazioni dai supporti di memorizzazione; (h) la tracciatura e la gestione degli eventi rilevanti ai fini della sicurezza e in base a quanto disposto dalle normative esterne di riferimento; (i) l'implementazione di adeguati meccanismi di isolamento dei dati gestiti dal FORNITORE per conto del CLIENTE, rispetto ai dati gestiti per conto di propri altri clienti a garanzia della loro riservatezza e integrità.

Uso sicuro dei sistemi del FORNITORE	
ID	Clausola
4.1	Il FORNITORE si impegna a garantire la gestione delle attività sottoelencate: (a) Se un incidenti di sicurezza effettivo o potenziale che coinvolge i sistemi del Fornitore ha provocato o può ragionevolmente comportare l'accesso o la divulgazione non autorizzati o avere effetti negativi materiali sui dati, informazioni riservate e infrastrutture del CLIENTE e/o dei suoi Clienti, o sistemi del Fornitore, il Fornitore compirà ogni ragionevole sforzo per informare immediatamente il CLIENTE di tale Incidente di sicurezza effettivo o potenziale, ma in ogni caso tale notifica avverrà entro 36 ore dalla data in cui il Fornitore verrà a conoscenza di tale incidente, salvo diverse indicazioni definite nelle specifiche tecniche del servizio. La notifica contiene almeno i seguenti dettagli: a. Data e ora dell'incidente di sicurezza. b. Un riepilogo di tutti i fatti rilevanti noti in relazione all'incidente di sicurezza c. Azioni intraprese dal Fornitore fino ad oggi per porre rimedio all'Incidente di Sicurezza e ad eventuali guasti che portano all'Incidente di Sicurezza d. Eventuali misure aggiuntive proposte dal Fornitore sono adottate dal Fornitore per porre rimedio agli effetti dell'Incidente di Sicurezza (b) rispettare i tempi di risposta agli incidenti di sicurezza concordati in Contratto, e comunque non oltre le 36 ore dal momento in cui il FORNITORE ne è venuto a conoscenza; (c) patch management di sicurezza eseguito con processi di aggiornamento controllati e tempi adeguati alla gravità delle vulnerabilità, non superiori a due mesi (secondo le previsioni di legge) ed inferiori a 5 giorni per i casi più gravi; (d) antivirus management eseguito con aggiornamento periodico conforme alle prescrizioni di corretto utilizzo del sistema antivirus adottato;

Uso sicuro dei sistemi del FORNITORE	
ID	Clausola
	(e) il fornitore garantisce l'installazione e la piena funzionalità di un sistema di protezione degli attacchi di tipo EDR/XDR (Endpoint Detection and Response) installato sui PC e sui Server del Fornitore monitorato H24 da un Security Operation Center (SOC); (f) Il Fornitore garantisce l'utilizzo di un sistema di AntiPhishing per la protezione email; (g) dismissione controllata degli asset con l'adozione di sistemi di cancellazione sicura delle informazioni dai supporti di memorizzazione.

Back up dei dati	
ID	Clausola
5.2	Il FORNITORE si impegna a conservare e a migrare i dati del CLIENTE e/o dei suoi Clienti in paesi specifici indicati dal CLIENTE stessa e, inoltre, si impegna a concordare con il CLIENTE e/o dei suoi Clienti l'identificazione del canale da utilizzare per l'instradamento/spostamento dei dati.
5.3	Il FORNITORE si impegna ad effettuare, se necessario, tutte le attività per garantire il ripristino totale del patrimonio ICT esposto ad un evento di sicurezza (ad es. backup dei dati), nei termini previsti nel contratto.
5.4	Il FORNITORE si impegna ad eseguire il backup periodico dei dati inerenti alle attività e ai processi inerenti al contratto. In particolare, deve garantire: (a) la conservazione delle copie di backup in un luogo sicuro e a prova di incendio e di intrusione; (b) la recovery dalle copie di backup e l'esecuzione di test di recovery dedicati con cadenza prefissata; (c) la conservazione delle copie dei dati oggetto del rapporto contrattuale; (d) la conservazione delle copie dei dati di configurazione dei sistemi e degli apparati che concorrono ad assicurare l'erogazione del servizio.

Tracciatura e conservazione dei Log File	
ID	Clausola
6.1	Il FORNITORE si impegna a eseguire in maniera sistematica e formalizzata, nel rispetto della legge: (a) la tracciatura applicativa per i software inerenti o riconducibili allo svolgimento delle prestazioni contrattuali; (b) la tracciatura per i sistemi e apparati inerenti o riconducibili al servizio oggetto del contratto Gli "event records" generati dai sistemi di autenticazione dovranno contenere riferimenti allo "username" utilizzato, alla data e all'ora dell'evento ("timestamp"), una descrizione dell'evento (ad es. sistema di elaborazione o software utilizzato; se si tratti di un evento di log-in, di log-out, o di una condizione di errore; quale linea di comunicazione o dispositivo terminale sia stato utilizzato), l'identificazione del sistema sul quale lo "username" ha operato. (c) i log di cui alle lettere (a) e (b) dovranno essere conservati per un periodo non inferiore a 6 mesi, e nel rispetto delle normative vigenti.
6.2	I risultati delle tracciature dovranno essere conservati con modalità sicure e auditabili, che garantiscano leggibilità, integrità e attendibilità ed esibiti a richiesta (anche richiesta diretta della funzione Audit del CLIENTE o da parte dei suoi Clienti).
6.3	Il FORNITORE assicura la piena ricostruzione degli accessi e delle modifiche effettuate sui dati, anche per finalità ispettive.

Sviluppo e manutenzione software	
ID	Clausola
7.1	Nel caso di attività di sviluppo o manutenzione software o che comunque comportino la scrittura/modifica di software utilizzato dal CLIENTE e/o dei suoi Clienti, il FORNITORE si impegna a utilizzare tecniche di sviluppo sicuro del software, che prevedano almeno l'implementazione della validazione dei dati in ingresso, controlli di validazione dell'elaborazione interna, controlli di validità dei messaggi e dell'output, l'utilizzo di best practice riferite allo specifico linguaggio di programmazione o ambiente che si utilizza per lo sviluppo. Per tutta la durata del Contratto, il FORNITORE si obbliga a rispettare le linee guida di codifica sicura del software elencate nel Progetto Open Web Application Security (OWASP), CWE TOP 25 Most Dangerous Software Errors SANS e atri standard di sicurezza.

Sviluppo e manutenzione software	
ID	Clausola
7.2	Nei limiti in cui le attività di cui sopra avvengano su ambienti gestiti dal FORNITORE, quest'ultimo è tenuto ad assicurare: (a) la separazione logica tra l'ambiente di produzione e gli altri ambienti; (b) che gli ambienti di sviluppo, test e produzione siano dedicati al CLIENTE e/o ai suoi Clienti, a garanzia della loro riservatezza ed integrità. (c) eseguire le attività di test in maniera tale da garantire la loro oggettività, verificabilità e ripetibilità; (d) non utilizzare i dati di produzione di proprietà del CLIENTE e/o dei suoi Clienti per le attività di test se non opportunamente anonimizzati; (e) realizzare una completa documentazione dei test effettuati in ambito sicurezza; (f) l'accesso a dati 'di produzione' o comunque a dati personali va contenuto ai casi di effettiva e reale necessità (ad es. manutenzione "correttiva in emergenza"), limitato al tempo strettamente necessario e comunque specificamente e preventivamente concordato.
7.3	Per i servizi Web Based o esposti sulla rete internet, sono richieste le seguenti misure di protezione da attacchi cyber: (a) protezione da attacchi DDOS; (b) Protezione da attacchi web tramite l'adozione di Web Application Firewall (WAF); (c) Protezione da attacchi di Brute force Password e Password Spray; (d) Utilizzo di sistemi di Multi Factor Authentication (MFA); (e) Esecuzione annuale di Penetration Test, con impegno a risolvere le eventuali vulnerabilità individuate in base al rischio.

Connessione ai sistemi gestiti dalla CLIENTE	
ID	Clausola
8.1	Nel caso di attività che richiedano la connessione di apparecchiature del FORNITORE alle reti e/o a sistemi gestiti dal CLIENTE, il FORNITORE si impegna a: (a) utilizzare unicamente reti d'accesso dedicate o comunque separate rispetto alla rete interna gestita dal CLIENTE; (b) accedere alle reti del CLIENTE esclusivamente connessioni sicure (es: VPN); (c) utilizzare tale connessione, come pure gli ID, le password ed in generale le "credenziali d'accesso" fornite, unicamente al fine dell'esecuzione delle attività strettamente inerenti alle attività contrattuali; (d) utilizzare esclusivamente postazioni di lavoro gestite in sicurezza.
8.2	Nei limiti in cui le attività di cui sopra avvengano su ambienti gestiti dal FORNITORE, quest'ultimo è tenuto ad assicurare: (e) la separazione logica tra l'ambiente di produzione e gli altri ambienti; (f) che gli ambienti di sviluppo, test e produzione siano dedicati al CLIENTE e/o ai suoi Clienti, a garanzia della loro riservatezza ed integrità. (g) eseguire le attività di test in maniera tale da garantire la loro oggettività, verificabilità e ripetibilità; (h) non utilizzare i dati di produzione di proprietà del CLIENTE e/o dei suoi Clienti per le attività di test se non opportunamente anonimizzati; (i) realizzare una completa documentazione dei test effettuati in ambito sicurezza; (j) l'accesso a dati 'di produzione' o comunque a dati personali va contenuto ai casi di effettiva e reale necessità (ad es. manutenzione "correttiva in emergenza"), limitato al tempo strettamente necessario e comunque specificamente e preventivamente concordato.
8.3	Il FORNITORE prende atto e accetta che il CLIENTE ha facoltà di monitorare gli accessi e l'utilizzo fatto della connessione, anche per ragioni di sicurezza o di regolarità e continuità operativa, e di chiedere informazioni sulle caratteristiche tecniche di tali apparecchiature.

Credenziali o strumenti della CLIENTE	
ID	Clausola
9.1	In tutti i casi in cui il FORNITORE sia stato dotato di credenziali o di strumenti informatici o di identificazione e di accesso (es. badge, chiavi, smart card, certificati digitali, ...) necessari per l'accesso ai sistemi dal CLIENTE stessa, il FORNITORE - nel rispetto delle normative vigenti - deve: (a) garantire la capacità e affidabilità del soggetto assegnatario in relazione all'incarico per il quale è richiesta l'assegnazione delle credenziali/strumenti; (b) curare istruire gli addetti affinchè le credenziali/strumenti siano custodite/i con la massima cura e non siano in alcun modo rese disponibili a terzi e siano utilizzate solo per lo svolgimento delle prestazioni contrattualmente previste; (c) istruire gli addetti affinchè che non ne siano fatte copie, salvo ove autorizzate dal CLIENTE; (d) assicurare che delle credenziali e strumenti sia fatto uso esclusivamente da parte dei soggetti assegnatari; in tutti i casi in cui – limitatamente ed in conformità alle regole, normative, standard e procedure aziendali vigenti – venga effettuato un cambio di assegnatario, verrà sottoscritto un documento per attestare tale cambiamento; (e) segnalarne tempestivamente al CLIENTE l'eventuale perdita di possesso (anche momentanea) come pure ogni possibile violazione delle norme di cui sopra; (f) segnalare al CLIENTE ogni altro evento (ad es. cessazione del rapporto di lavoro; modifica delle mansioni), che determini il venir meno della necessità di disporre di tali credenziali o strumenti.

Attività relative all'hardware – servizi sistemistici e TLC	
ID	Clausola
10.1	In caso di ritiro o sostituzione di apparecchiature informatiche rese disponibili dal FORNITORE e utilizzate dal CLIENTE e/o di memorie di qualunque tipo che possano contenere programmi per elaborare o dati del CLIENTE e/o dei suoi Clienti, tutti i dati contenuti nelle memorie sostituite dovranno essere cancellati in modo irreversibile a cura del FORNITORE, previo inserimento dei dati sulla nuova apparecchiatura o su idoneo supporto, secondo le richieste del CLIENTE.
10.2	In tutte le attività di manutenzione, come pure nei servizi sistemistici e di gestione delle reti, dovranno essere prese - in coordinamento con il CLIENTE - misure per prevenire la perdita anche accidentale di dati, anche residenti su apparecchiature diverse da quelle sulle quali si esegue l'intervento.

Amministratori di Sistema	
ID	Clausola
11.1	Il FORNITORE è tenuto a mantenere una lista aggiornata degli "amministratori di sistema" abilitati ad operare sui dati o sui sistemi del CLIENTE e/o dei suoi Clienti ed a comunicarne gli estremi su richiesta e/o secondo le periodicità concordate.
11.2	Il FORNITORE è tenuto ad effettuare le necessarie verifiche preventive di affidabilità, nonché le verifiche periodiche previste dalla normativa, dandone conto secondo necessità.

Audit e verifiche	
ID	Clausola
12.2	Il CLIENTE ha la facoltà di condurre audit diretto e/o a procedere a richieste di informazioni previste dalla legge o dal Contratto, sia in caso di incidente di sicurezza sia come parte di una verifica periodica del rispetto delle disposizioni normative e contrattuali.
12.3	Il FORNITORE deve prestare l'opportuna collaborazione all'effettuazione dell'audit e comunque consentire che i soggetti indicati al comma precedente possano intervistare il proprio staff (nel rispetto delle leggi e dei regolamenti vigenti) e possano accedere a: (a) tutte le informazioni e i documenti relativi ai servizi; (b) ai sistemi, strumenti, network, ai database, ai piani di continuità operativa, e altre informazioni relative ai servizi; (c) alle strutture e i locali dove il servizio viene erogato.
12.4	Il FORNITORE si impegna, ove richiesto, a predisporre gli opportuni remediation plan per eliminare eventuali non conformità riscontrate nei tempi concordati.

Requisiti di sicurezza aggiuntivi per l'esternalizzazione di servizi in cloud In caso di esternalizzazione di servizio/soluzione in cloud, in aggiunta alle clausole riportate nei precedenti paragrafi, devono essere garantiti almeno i seguenti requisiti	
ID	Clausola
13.1	Nel caso di risoluzione del Contratto, il FORNITORE si impegna a supportare il CLIENTE nella gestione dell'exit strategy attraverso il trasferimento dei dispositivi, sistemi, dati ad un Fornitore terzo o supportando il re-insourcing dell'attività.
13.2	Il FORNITORE si impegna ad implementare i controlli di sicurezza specificati nella matrice dei controlli cloud previsti dal CLIENTE, definiti nel framework CSA CCM (Cloud Security Alliance Cloud Controls Matrix). Inoltre, il FORNITORE si impegna a fornire, su richiesta del CLIENTE, la documentazione e le evidenze necessarie a dimostrarne la conformità.
13.3	Il FORNITORE si impegna, qualora (anche successivamente alla stipula del Contratto) venga meno la possibilità di implementare un controllo della matrice dei controlli cloud, ad informare tempestivamente il CLIENTE.
13.4	Il FORNITORE si impegna a predisporre specifica documentazione che descriva le procedure di gestione interna delle modifiche in produzione ed i relativi ruoli/diritti/responsabilità all'interno del Cloud.
13.5	Il FORNITORE si impegna ad implementare metodi di crittografia aperti (AES, ecc.) per proteggere i dati nel caso in cui debbano attraversare reti pubbliche (ad es. Internet).

Vulnerability Assessment e Penetration Test	
ID	Clausola
14.1	Il FORNITORE deve garantire l'esecuzione di attività di Vulnerability Assessment interne con cadenza almeno annuale sul perimetro di pertinenza dei servizi erogati al CLIENTE e/o ai suoi Clienti.
14.2	Il FORNITORE deve garantire l'esecuzione di attività di Penetration Test interne con cadenza almeno annuale, sul perimetro di pertinenza dei servizi erogati al CLIENTE e/o ai suoi Clienti.
14.3	Il FORNITORE deve inoltre riconoscere al CLIENTE il diritto di visionare su richiesta della stessa i risultati dei test delle attività di Vulnerability Assessment e Penetration Test svolte internamente sul perimetro di pertinenza dei servizi erogati al CLIENTE e/o ai suoi Clienti.